

Re: My Solution to Securing Windows 98, ME Against Network Modification and Spying, using Linux.

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-05/1667.html>

From: Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP] (sbradcpa_at_pacbell.net)

Date: 05/28/03

Date: Tue, 27 May 2003 19:41:50 -0700

The Five Worst Security Mistakes End Users Make

Failing to install anti-virus, keep its signatures up to date, and apply it to all files.

Opening unsolicited e-mail attachments without verifying their source and checking their content first, or executing games or screen savers or other programs from untrusted sources.

Failing to install security patches—especially for Microsoft Office, Microsoft Internet Explorer, and Netscape.

Not making and testing backups.

Using a modem while connected through a local area network.

The Seven Worst Security Mistakes Senior Executives Make

Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job.

Failing to understand the relationship of information security to the business problem—they understand physical security but do not see the consequences of poor information security.

Failing to deal with the operational aspects of security: making a few fixes and then not allowing the follow through necessary to ensure the problems stay fixed

Relying primarily on a firewall.

Failing to realize how much money their information and organizational reputations are worth.

Authorizing reactive, short-term fixes so problems re-emerge rapidly.

Pretending the problem will go away if they ignore it.

The Ten Worst Security Mistakes Information Technology People Make

Connecting systems to the Internet before hardening them.

Connecting test systems to the Internet with default accounts/passwords

Failing to update systems when security holes are found.

Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI.

Giving users passwords over the phone or changing user passwords in response to

Re: My Solution to Securing Windows 98, ME Against Network Modification and Spying, using Linux.

telephone or personal requests when the requester is not authenticated.

Failing to maintain and test backups.

Running unnecessary services, especially ftpd, telnetd, finger, rpc, mail, rservices

Implementing firewalls with rules that don't stop malicious or dangerous traffic—incoming or outgoing.

Failing to implement or update virus detection software

Failing to educate users on what to look for and what to do when they see a potential security problem.

And a bonus, number 11: Allowing untrained, uncertified people to take responsibility for securing important systems.

Simon wrote:

- > *As a security consultant I have seen more so called administrators creating*
- > *security risks than users. So should that be SCA. It's easy to blame the*
- > *user but if the administrators don't understand security and don't create an*
- > *environment in which the risks are reduced how can you expect a user to know*
- > *any better.*
- > *What about Security Awareness, Policy, Procedure, Best Practise etc.*
- >
- > *Simon*
- >
- > *"Susan Bradley, CPA aka Ebitz SBS Rocks [MVP]" <sbradcpa@pacbell.net> wrote*
- > *in message news:3ED15511.11CF9E08@pacbell.net...*
- > *> SCU's. SCU's are the bane of every company, cause all security issues,*
- > *> all vulnerabilities, and are the root of most security issues..... what are*
- > *> SCU's? Stupid Computer Users. They open email attachments, the don't*
- > *> update their A/V software, they want to run Kazaa in their system, they*
- > *> download spyware programs....etc...etc...*
- > >